Nonuniform Coercions via Unification Hints

Claudio Sacerdoti Coen[1], Enrico Tassi[2]

[1]University of Bologna - Department of Computer Science
[2]Microsoft Research-INRIA Joint Center

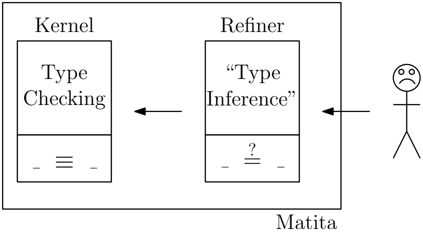
TYPES 2010 — 15 October 2010 — Warsaw

Context of this work

- Interactive theorem prover Matita (CIC)
- Formalization of formal topology (Algebraic Structures)

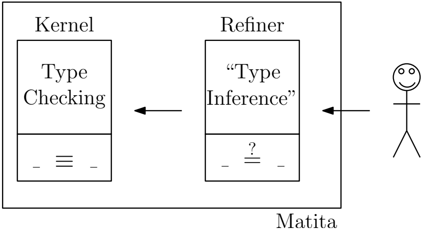
Context of this work

- Interactive theorem prover Matita (CIC)
- Formalization of formal topology (Algebraic Structures)



Context of this work

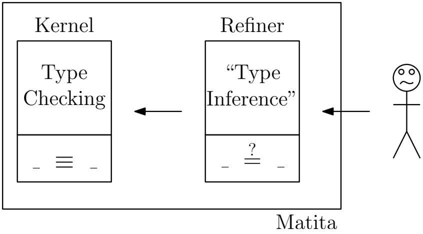
- Interactive theorem prover Matita (CIC)
- Formalization of formal topology (Algebraic Structures)



- Unification made user-extensible (Unification Hints)

Context of this work

- Interactive theorem prover Matita (CIC)
- Formalization of formal topology (Algebraic Structures)



- Unification made user-extensible (Unification Hints)
- In some corner cases the system is unable to exploit the knowledge given by hints

Example

record Group : Type := { carr : Type, $\_*\_$: ...}
definition $\mathcal{Z}$: Group := $\langle$ Z, +, 0, ...$\rangle$.
lemma mulg1: $\forall$ G:Group, $\forall$ a:carr G. $a * 1 = a$.
lemma cardG_gt0 : $\forall$ G : Group, $0 < |G|$.

check (mulg1 $?_G$ 2).

Example

record Group : Type := { carr : Type, _*_ : ...}
definition $\mathcal{Z}$: Group := ⟨ Z, +, 0, ...⟩.
lemma mulg1: ∀ G:Group, ∀ a:carr G. a ∗ 1 = a.
lemma cardG_gt0 : ∀ G : Group, 0 < |G|.

check (mulg1 $?_G$ 2).

Works, since 2 has type Z, and it's context expects a term of type carr $?_G$ and the unification algorithm knows a canonical solution for Z $\stackrel{?}{=}$ carr $?_G$.

Example

record Group : Type := { carr : Type, _∗_ : ...}
definition $\mathcal{Z}$: Group := ⟨ Z, +, 0, ...⟩.
lemma mulg1: ∀ G:Group, ∀ a:carr G. a ∗ 1 = a.
lemma cardG_gt0 : ∀ G : Group, 0 < |G|.

check (mulg1 $?_G$ 2).

Works, since 2 has type Z, and it's context expects a term of type carr $?_G$ and the unification algorithm knows a canonical solution for Z $\stackrel{?}{=}$ carr $?_G$.

check (cardG_gt0 Z).

Example

record Group : Type := { carr : Type, _*_ : ...}
definition $\mathcal{Z}$: Group := ⟨ Z, +, 0, ...⟩.
lemma mulg1: ∀ G:Group, ∀ a:carr G. a ∗ 1 = a.
lemma cardG_gt0 : ∀ G : Group, 0 < |G|.

check (mulg1 $?_G$ 2).

Works, since 2 has type Z, and it's context expects a term of type carr $?_G$ and the unification algorithm knows a canonical solution for Z $\stackrel{?}{=}$ carr $?_G$.

check (cardG_gt0 Z).

Error: Z has type Type but it's context expects a term of type Group. The unification problem Type $\stackrel{?}{=}$ Group has no solution.

Outline

1. Coercions
    - Nonuniform coercions
    - Examples
2. Implementation
    - Ingredients
    - Declaring nonuniform coercions
    - Reusing existing hints
3. Conclusions

Type inference and coercions

- These problems have to be addressed by type inference

$$\Gamma \vdash t : T \rightsquigarrow t' : T'$$

- Looks like coercions could solve these typing errors

$$\frac{}{\Gamma \vdash x : N \rightsquigarrow \qquad : Z}$$

Type inference and coercions

- These problems have to be addressed by type inference

$$\Gamma \vdash t : T \leadsto t' : T'$$

- Looks like coercions could solve these typing errors

$$\frac{(k, (N, Z)) \in \Delta}{\Gamma \vdash x : N \leadsto \qquad : Z}$$

Type inference and coercions

- These problems have to be addressed by type inference

$$\Gamma \vdash t : T \leadsto t' : T'$$

- Looks like coercions could solve these typing errors

$$\frac{(k, (N, Z)) \in \Delta}{\Gamma \vdash x : N \leadsto \qquad : Z}$$

Type inference and coercions

- These problems have to be addressed by type inference

$$\Gamma \vdash t : T \rightsquigarrow t' : T'$$

- Looks like coercions could solve these typing errors

$$\frac{(k, (N, Z)) \in \Delta}{\Gamma \vdash x : N \rightsquigarrow : Z}$$

Type inference and coercions

- These problems have to be addressed by type inference

$$\Gamma \vdash t : T \rightsquigarrow t' : T'$$

- Looks like coercions could solve these typing errors

$$\frac{(k, (N, Z)) \in \Delta \qquad \Gamma \vdash k\ x : Z}{\Gamma \vdash x : N \rightsquigarrow \qquad : Z}$$

Type inference and coercions

- These problems have to be addressed by type inference

$$\Gamma \vdash t : T \rightsquigarrow t' : T'$$

- Looks like coercions could solve these typing errors

$$\frac{(k,(N,Z)) \in \Delta \quad \Gamma \vdash k\ x : Z \quad Z \stackrel{?}{=} Z}{\Gamma \vdash x : N \rightsquigarrow \qquad : Z}$$

Type inference and coercions

- These problems have to be addressed by type inference

$$\Gamma \vdash t : T \rightsquigarrow t' : T'$$

- Looks like coercions could solve these typing errors

$$\frac{(k, (N, Z)) \in \Delta \qquad \Gamma \vdash k\ x : Z \qquad Z \stackrel{?}{=} Z}{\Gamma \vdash x : N \rightsquigarrow k\ x : Z}$$

Type inference and coercions

- These problems have to be addressed by type inference

$$\Gamma \vdash t : T \rightsquigarrow t' : T'$$

- Looks like coercions could solve these typing errors

$$\frac{(k,(N,Z)) \in \Delta \quad \Gamma \vdash k\ x : Z \quad Z \stackrel{?}{=} Z}{\Gamma \vdash x : N \rightsquigarrow k\ x : Z}$$

- but (uniform) coercions are type theoretic functions whose insertion is type driven.

$$\frac{(\lambda\_.\mathcal{Z},(\mathit{Type},\mathit{Group})) \in \Delta \quad \Gamma \vdash (\lambda\_.\mathcal{Z})\ Z : \mathit{Group}}{\Gamma \vdash Z : \mathit{Type} \rightsquigarrow (\lambda\_.\mathcal{Z})\ Z : \mathit{Group}}$$

Type inference and coercions

- These problems have to be addressed by type inference

$$\Gamma \vdash t : T \leadsto t' : T'$$

- Looks like coercions could solve these typing errors

$$\frac{(k, (N, Z)) \in \Delta \qquad \Gamma \vdash k\ x : Z \qquad Z \stackrel{?}{=} Z}{\Gamma \vdash x : N \leadsto k\ x : Z}$$

- but (uniform) coercions are type theoretic functions whose insertion is type driven.

$$\frac{(\lambda\_.\mathcal{Z}, (Type, Group)) \in \Delta \qquad \Gamma \vdash (\lambda\_.\mathcal{Z})\ Q : Group}{\Gamma \vdash Q : Type \leadsto (\lambda\_.\mathcal{Z})\ Q : Group}$$

Nonuniform coercions

$$\Delta = \left\{ \Gamma_1 \vdash \begin{array}{ccc} S_1 & \to & T_1 \\ s_1 & \mapsto & t_1 \end{array} \quad \ldots \quad \Gamma_n \vdash \begin{array}{ccc} S_n & \to & T_n \\ s_n & \mapsto & t_n \end{array} \right\}$$

where

$$\Gamma_i \vdash s_i : S_i \qquad \Gamma_i \vdash t_i : T_i$$

Inserting a nonuniform coercion works as follows:

$$\frac{}{\Gamma \vdash s : S \rightsquigarrow \quad : T}$$

where variables in Γ_i are replaced by unification variables.

Nonuniform coercions

$$\Delta = \left\{ \quad \Gamma_1 \;\vdash\; \begin{array}{ccc} S_1 & \to & T_1 \\ s_1 & \mapsto & t_1 \end{array} \quad \ldots \quad \Gamma_n \;\vdash\; \begin{array}{ccc} S_n & \to & T_n \\ s_n & \mapsto & t_n \end{array} \quad \right\}$$

where

$$\Gamma_i \vdash s_i : S_i \qquad \Gamma_i \vdash t_i : T_i$$

Inserting a nonuniform coercion works as follows:

$$\frac{\left(\Gamma_i \vdash \begin{array}{ccc} S_i & \to & T_i \\ s_i & \mapsto & t_i \end{array} \right) \in \Delta}{\Gamma \vdash s : S \leadsto \quad : T}$$

where variables in Γ_i are replaced by unification variables.

Nonuniform coercions

$$\Delta = \left\{ \quad \Gamma_1 \quad \vdash \quad \begin{matrix} S_1 & \rightarrow & T_1 \\ s_1 & \mapsto & t_1 \end{matrix} \quad \ldots \quad \Gamma_n \quad \vdash \quad \begin{matrix} S_n & \rightarrow & T_n \\ s_n & \mapsto & t_n \end{matrix} \quad \right\}$$

where

$$\Gamma_i \vdash s_i : S_i \qquad \Gamma_i \vdash t_i : T_i$$

Inserting a nonuniform coercion works as follows:

$$\frac{\left(\Gamma_i \vdash \begin{matrix} S_i & \rightarrow & T_i \\ s_i & \mapsto & t_i \end{matrix} \right) \in \Delta \qquad S \stackrel{?}{=} S_i}{\Gamma \vdash s : S \rightsquigarrow \quad : T}$$

where variables in Γ_i are replaced by unification variables.

Nonuniform coercions

$$\Delta = \left\{ \Gamma_1 \vdash \begin{array}{ccc} S_1 & \to & T_1 \\ s_1 & \mapsto & t_1 \end{array} \quad \ldots \quad \Gamma_n \vdash \begin{array}{ccc} S_n & \to & T_n \\ s_n & \mapsto & t_n \end{array} \right\}$$

where

$$\Gamma_i \vdash s_i : S_i \qquad \Gamma_i \vdash t_i : T_i$$

Inserting a nonuniform coercion works as follows:

$$\frac{\left(\Gamma_i \vdash \begin{array}{ccc} S_i & \to & T_i \\ s_i & \mapsto & t_i \end{array}\right) \in \Delta \qquad \begin{array}{ccc} S & \stackrel{?}{=} & S_i \\ s & \stackrel{?}{=} & s_i \end{array}}{\Gamma \vdash s : S \leadsto \quad : T}$$

where variables in Γ_i are replaced by unification variables.

Nonuniform coercions

$$\Delta = \left\{ \quad \Gamma_1 \;\vdash\; \begin{array}{ccc} S_1 & \to & T_1 \\ s_1 & \mapsto & t_1 \end{array} \quad \ldots \quad \Gamma_n \;\vdash\; \begin{array}{ccc} S_n & \to & T_n \\ s_n & \mapsto & t_n \end{array} \quad \right\}$$

where

$$\Gamma_i \vdash s_i : S_i \qquad \Gamma_i \vdash t_i : T_i$$

Inserting a nonuniform coercion works as follows:

$$\frac{\left(\Gamma_i \vdash \begin{array}{ccc} S_i & \to & T_i \\ s_i & \mapsto & t_i \end{array} \right) \in \Delta \qquad \begin{array}{ccc} S & \stackrel{?}{=} & S_i \\ s & \stackrel{?}{=} & s_i \\ T & \stackrel{?}{=} & T_i \end{array}}{\Gamma \vdash s : S \leadsto \quad : T}$$

where variables in Γ_i are replaced by unification variables.

Nonuniform coercions

$$\Delta = \left\{ \quad \Gamma_1 \quad \vdash \quad \begin{matrix} S_1 & \rightarrow & T_1 \\ s_1 & \mapsto & t_1 \end{matrix} \quad \ldots \quad \Gamma_n \quad \vdash \quad \begin{matrix} S_n & \rightarrow & T_n \\ s_n & \mapsto & t_n \end{matrix} \quad \right\}$$

where

$$\Gamma_i \vdash s_i : S_i \qquad \Gamma_i \vdash t_i : T_i$$

Inserting a nonuniform coercion works as follows:

$$\frac{\left(\Gamma_i \vdash \begin{matrix} S_i & \rightarrow & T_i \\ s_i & \mapsto & t_i \end{matrix} \right) \in \Delta \qquad \begin{matrix} S & \stackrel{?}{=} & S_i \\ s & \stackrel{?}{=} & s_i \\ T & \stackrel{?}{=} & T_i \end{matrix}}{\Gamma \vdash s : S \rightsquigarrow t_i : T}$$

where variables in Γ_i are replaced by unification variables.

Nonuniform coercions: examples

Uniform coercions

$$x : N \;\vdash\; \begin{array}{ccc} N & \rightarrow & Z \\ x & \mapsto & k\ x \end{array}$$

Nonuniform coercions

$$\vdash\; \begin{array}{ccc} Type & \rightarrow & Group \\ Z & \mapsto & \mathcal{Z} \end{array}$$

$$\vdash\; \begin{array}{ccc} Type & \rightarrow & Group \\ Q & \mapsto & \mathcal{Q} \end{array}$$

Cheap implementation: ingredient #1

Unification hints:

$$\Gamma \vdash \frac{\overrightarrow{?_x} \;:=\; \overrightarrow{H}}{P \;\equiv\; Q}\ \text{myhint}$$

Cheap implementation: ingredient #1

Unification hints:

$$\Gamma \vdash \frac{\overrightarrow{?_x} \ := \ \overrightarrow{H}}{P \ \equiv \ Q} \text{ myhint}$$

Examples:

$$\vdash \frac{?_G \ := \ \mathcal{Z}}{Z \ \equiv \ carr \ ?_G}$$

Cheap implementation: ingredient #1

Unification hints:

$$\Gamma \vdash \frac{\overrightarrow{?_x} \;:=\; \overrightarrow{H}}{P \;\equiv\; Q}\ \text{myhint}$$

Examples:

$$\vdash \frac{?_G \;:=\; \mathcal{Z}}{Z \;\equiv\; carr\ ?_G}$$

$$G, H : Group \vdash \frac{\begin{array}{rcl} ?_A & := & carr\ \ G \\ ?_B & := & carr\ \ H \\ ?_X & := & product\_group\ \ G\ \ H \end{array}}{?_A \;\times\; ?_B \;\equiv\; carr\ ?_X}$$

Cheap implementation: ingredient #1 (cont.)

Note that hints define "equivalence classes" of constants, thus approximated indexing for fast retrieval must take them into account.

$$\frac{(k,(N,Z)) \in \Delta \quad \Gamma \vdash k\ s : Z \quad Z \stackrel{?}{=} carr\ \mathcal{Z}}{\Gamma \vdash s : N \leadsto k\ s : carr\ \mathcal{Z}}$$

Cheap implementation: ingredient #1 (cont.)

Note that hints define "equivalence classes" of constants, thus approximated indexing for fast retrieval must take them into account.

$$\frac{(k,(N,Z)) \in \Delta \quad \Gamma \vdash k\ s : Z \quad Z \stackrel{?}{=} carr\ \mathcal{Z}}{\Gamma \vdash s : N \leadsto k\ s : carr\ \mathcal{Z}}$$

Cheap implementation: ingredient #2

Uniform coercion loosely indexed:

$$\frac{(\mathit{result}, (*, \mathit{target})) \in \Delta \qquad \Gamma \vdash \mathit{result}\ s : \mathit{target} \qquad \mathit{target} \stackrel{?}{=} T}{\Gamma \vdash x : S \rightsquigarrow \mathit{result}\ s : T}$$

Note that T and *target* can be in the same equivalence class.

Encoding nonuniform coercions

record solution (S : Type) (s : S) : Type :={
  target : Type; *(* T *)*
  result : target *(* t *)*
}.

coercion result : ∀S:Type.∀s:S.∀sol:solution S s. target S s sol
on s : ? $\rightarrowtail$ target ???.

Encoding nonuniform coercions

```
record solution (S : Type) (s : S) : Type :={
   target : Type;      (* T *)
   result : target     (* t *)
}.

coercion result : ∀S:Type.∀s:S.∀sol:solution S s. target S s sol
on s : ? >—> target ???.
```

$$s \rightsquigarrow result\ ?\ s\ ?_{sol}$$

Declaring nonuniform coercions

$$\vdash \begin{array}{lcl} Type & \rightarrow & Group \\ Z & \mapsto & \mathcal{Z} \end{array}$$

$$\frac{}{\Gamma \vdash Z : Type \rightsquigarrow \qquad\qquad : Group}$$

Declaring nonuniform coercions

$$\vdash \begin{array}{lll} Type & \to & Group \\ Z & \mapsto & \mathcal{Z} \end{array}$$

$$(result, (*, target)) \in \Delta$$

$$\frac{}{\Gamma \vdash Z : Type \rightsquigarrow \qquad\qquad : Group}$$

Declaring nonuniform coercions

$$\vdash \begin{array}{lcl} \mathit{Type} & \rightarrow & \mathit{Group} \\ Z & \mapsto & \mathcal{Z} \end{array}$$

$$(\mathit{result}, (*, \mathit{target})) \in \Delta$$

$$\frac{}{\Gamma \vdash Z : \mathit{Type} \rightsquigarrow \qquad\qquad : \mathit{Group}}$$

Declaring nonuniform coercions

$$\vdash \begin{array}{lcl} \mathit{Type} & \to & \mathit{Group} \\ Z & \mapsto & \mathcal{Z} \end{array}$$

$$(\mathit{result}, (*, \mathit{target})) \in \Delta$$

$$\frac{}{\Gamma \vdash Z : \mathit{Type} \leadsto \qquad\qquad : \mathit{Group}}$$

Declaring nonuniform coercions

$$\vdash \begin{array}{lcl} Type & \to & Group \\ Z & \mapsto & \mathcal{Z} \end{array}$$

$$\frac{(result, (*, target)) \in \Delta \qquad \Gamma \vdash result\ ?\ Z\ ?_{sol} : target\ \ Type\ Z\ ?_{sol}}{\Gamma \vdash Z : Type \rightsquigarrow \qquad\qquad : Group}$$

Declaring nonuniform coercions

$$\vdash \quad \begin{array}{lcl} Type & \to & Group \\ Z & \mapsto & \mathcal{Z} \end{array}$$

$$\frac{\begin{array}{c}(result, (*, target)) \in \Delta \\ \Gamma \vdash result\ ?\ Z\ ?_{sol} : target\ \ Type\ \ Z\ ?_{sol} \\ target\ \ Type\ \ Z\ ?_{sol} \stackrel{?}{=} Group\end{array}}{\Gamma \vdash Z : Type \rightsquigarrow \qquad\qquad : Group}$$

Declaring nonuniform coercions

$$\vdash \quad \begin{array}{lcl} \mathit{Type} & \to & \mathit{Group} \\ Z & \mapsto & \mathcal{Z} \end{array}$$

$$\frac{(\mathit{result}, (*, \mathit{target})) \in \Delta \qquad \Gamma \vdash \mathit{result}\ ?\ Z\ ?_{sol} : \mathit{target}\ \ \mathit{Type}\ Z\ ?_{sol} \qquad \mathit{target}\ \ \mathit{Type}\ Z\ ?_{sol} \stackrel{?}{=} \mathit{Group}}{\Gamma \vdash Z : \mathit{Type} \leadsto \mathit{result}\ ?\ Z\ ?_{sol} : \mathit{Group}}$$

Declaring nonuniform coercions

$$\vdash \begin{array}{lll} Type & \rightarrow & Group \\ Z & \mapsto & \mathcal{Z} \end{array}$$

$$\frac{\begin{array}{c}(result, (*, target)) \in \Delta \\ \Gamma \vdash result\ ?\ Z\ ?_{sol} : target\ \ Type\ Z\ ?_{sol} \\ target\ \ Type\ Z\ ?_{sol} \stackrel{?}{=} Group\end{array}}{\Gamma \vdash Z : Type \leadsto result\ ?\ Z\ ?_{sol} : Group}$$

We declare the following hint:

$$\vdash \frac{?_{sol}\ := \ mk\_solution\ Type\ Z\ Group\ \mathcal{Z}}{target\ \ Type\ Z\ ?_{sol}\ \equiv\ Group}$$

Declaring nonuniform coercions

$$\vdash \begin{array}{lcl} \mathit{Type} & \rightarrow & \mathit{Group} \\ Z & \mapsto & \mathcal{Z} \end{array}$$

$$\frac{\begin{array}{c}(\mathit{result}, (*, \mathit{target})) \in \Delta \\ \Gamma \vdash \mathit{result}\ ?\ Z\ ?_{sol} : \mathit{target}\ \ \mathit{Type}\ Z\ ?_{sol} \\ \mathit{target}\ \ \mathit{Type}\ Z\ ?_{sol} \stackrel{?}{=} \mathit{Group}\end{array}}{\Gamma \vdash Z : \mathit{Type} \rightsquigarrow \mathit{result}\ ?\ Z\ ?_{sol} : \mathit{Group}}$$

We declare the following hint:

$$\vdash \frac{?_{sol}\ \ :=\ \ \mathit{mk\_solution}\ \ \mathit{Type}\ \ Z\ \ \mathit{Group}\ \ \mathcal{Z}}{\mathit{target}\ \ \mathit{Type}\ Z\ ?_{sol}\ \ \equiv\ \ \mathit{Group}}$$

Note that:

$$\mathit{target}\ \ \mathit{Type}\ Z\ ?_{sol} \triangleright \mathit{Group}$$

Declaring nonuniform coercions

$$\vdash \begin{array}{lcl} Type & \to & Group \\ Z & \mapsto & \mathcal{Z} \end{array}$$

$$\frac{\begin{array}{c}(result, (*, target)) \in \Delta \\ \Gamma \vdash result\ ?\ Z\ ?_{sol} : target\ \ Type\ \ Z\ ?_{sol} \\ target\ \ Type\ \ Z\ ?_{sol} \stackrel{?}{=} Group\end{array}}{\Gamma \vdash Z : Type \leadsto result\ ?\ Z\ ?_{sol} : Group}$$

We declare the following hint:

$$\vdash \frac{?_{sol} \ := \ mk\_solution\ \ Type\ \ Z\ \ Group\ \ \mathcal{Z}}{target\ \ Type\ \ Z\ ?_{sol} \ \equiv \ Group}$$

Note that:

$$target\ \ Type\ \ Z\ ?_{sol} \triangleright Group \qquad result\ \ Type\ \ Z\ ?_{sol} \triangleright \mathcal{Z}$$

Declaring nonuniform coercions (the right way)

This is unsatisfactory, we need one new hint per coercion

$$\vdash \frac{?_{sol} \;:=\; mk\_solution\ Type\ Z\ Group\ \mathcal{Z}}{target\ Type\ Z\ ?_{sol} \;\equiv\; Group}$$

Moreover, the system is already aware that

$$\Gamma \vdash \frac{?_G \;:=\; \mathcal{Z}}{Z \;\equiv\; carr\ ?_G}$$

We need only this hint:

$$G : Group \vdash \frac{\begin{array}{lcl} ?_Z & := & carr\ G \\ ?_{sol} & := & mk\_solution\ Type\ ?_Z\ Group\ G \end{array}}{target\ Type\ ?_Z\ ?_{sol} \;\equiv\; Group}$$

Conclusion

Nonuniform coercions:

- Generalization of type-theoretic coercions
- Cheap implementation on top of unification hints
- Both type inference and unification can exploit the knowledge expressed in terms of Unification Hints

Conclusion

Nonuniform coercions:

- Generalization of type-theoretic coercions
- Cheap implementation on top of unification hints
- Both type inference and unification can exploit the knowledge expressed in terms of Unification Hints

Further research:

- Notion of coherence (sanity check on Δ as a whole)
- Notion of composition for nonuniform coercions

Thanks

Thanks for your attention!